REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-4 are pending in the application; Claims 5 and 7 having previously been withdrawn from consideration. Claims 1 and 4 are amended by the present amendment. Support for amended independent Claims 1 and 4 can be found in the original specification, claims, and drawings.[1] No new matter is presented.

In the outstanding Official Action, Claims 1-4 were rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent Publication No. 2003/0177391 to Ofek et al. (hereinafter Ofek).

Regarding the rejection of Claims 1-4, Applicant respectfully submits that amended independent Claims 1 and 4 recite novel features clearly not taught or rendered obvious by the applied references.

Amended independent Claim 1 relates to a sending apparatus that includes a means for sequentially sending packet data generated based on a predetermined communication protocol via a network. The sending apparatus comprises in part:

> ... means for ***receiving a request from a receiver device*** to add identification information to said sent packet data ***only during a predetermined period***; and
>
> means for adding said requested identification information to said sent packet data during said predetermined period and ***not adding identification information during periods other than said predetermined period*** ...

Independent Claim 4, while directed to an alternative embodiment, is amended to recite substantially similar features. Accordingly, the remarks and arguments presented below are applicable to each of independent Claims 1 and 4.

The claimed invention relates to a data sending/receiving system for responding to a denial of service (DoS) attack launched on a receiving device. A DoS occurs when an

[1] E.g., specification, Figs. 7 and 8 and corresponding description in the specification.

interfering apparatus intercepts valid packets of data sent from an authorized sending apparatus to a receiving apparatus, copies or modifies these packets of data, and then sends mass amounts of unauthorized traffic to the receiving apparatus to impair this device's ability to process authorized packets of received data.

The claimed invention is directed to a system that allows the receiver to request that the authorized sending apparatus attach identification information to each transmitter packet only when a DoS attack is detected. Thus, when the receiver does not detect a DoS attack, the authorized sending devices send packet data free of any identification information relieving the receiver from processing such data. However, when the receiving apparatus detects a DoS attack, a message is transmitted from the receiver to the sender requesting that the authorized sender attach identification to each packet of data transmitted to the receiver.

Turning to the applied reference, Ofek describes a method that provides a network interface with the capability to determine the authenticity of programs used to generate and send data packets, thereby ensuring the users who send data packets are well behaved.[2] A hidden program in the transmitter generates a pseudo-random number and the transmitter generates a pseudo-random sequence of security signals that are included in the sequence of data packets sent from the user to the network interface and only the network interface knows how the pseudo-random sequence of security signals was generated, and therefore, the network interface is able to check the validity of the pseudo-random sequence of security signals and verify the authenticity of the programs used to generate and send packets.[3]

Ofek, however, fails to teach or suggest receiving a request from a receiver device to add identification information to sent packet data "***only during a predetermined period***", and "***not adding identification information during periods other than said predetermined period***," as recited in amended independent Claim 1.

---

[2] Ofek, Abstract.
[3] Id.

In addressing the feature directed to receiving a request from a receiver to add identification information, the outstanding Official Action relies on paragraphs [0073], [0087] and [0103] and Fig. 6 of Ofek noting that "packets with security tags are sent sending (sic) in response to time stamps during predetermined time intervals."[4] This cited portion of Ofek describes that a general protocol is defined between the sources and a network interface, wherein the source contains a program for generating and sending data packets called trusted flow generated (TFG) and the network interface includes a program called security tag checker (TTC) for receiving and checking data packets. The data packets sent by TFG contain a security tag (111), which is part of the data packet header or part of the data packet pay load. Ofek further describes that the controller can send secure time-stamps (421) to the hidden program portion of the source, which are used by the hidden program portion to uniquely generate security signals. Thus, as noted in the Official Action, these secure time-stamps (421) may be used to generate proper security signals at the source. Further, as discussed at paragraph [0085] the hidden program portion (414) at the source initiates this exchange by sending a first security signal (411) to the controller for selectively coupling the data packets to the network interface. The coupling operation is performed responsive to the security signals (411), wherein the security signal (411) is part of the data packet.

Ofek, however, fails to teach or suggest "***not adding identification information during periods other than said predetermined period***" wherein said predetermine period is defined by a ***request received from the receiver device*** as recited in amended independent Claim 1.

Instead, as discussed at paragraph [0076] of Ofek, the data packets sent from the source are sent with security tags (111) wherein each has a size of at least one bit of information. Ofek fails to teach or suggest a scenario in which the security tags are not

[4] Official Action, p. 3.

generated and transmitted with the data packets. Further, paragraph [0073] of Ofek describes that in general, TFG does not have to attach the security tag (111) to every data packet, but only to predefine selected ones. Ofek, however, fails to teach or suggest that these packets are selected based on a request received from a receiver device and that identification information is not added during periods other than said predetermined period, as recited in amended independent Claim 1.

This understanding of Ofek is further supported by the description at paragraphs [0085]-[0087], which clearly describes that the process of adding security tags to data packets is generated by the TFG in the source station and facilitated by the network interface, or receiver. The addition of data packets, therefore, is not based on a request from a receiver device, whatsoever, as recited in amended independent Claim 1.

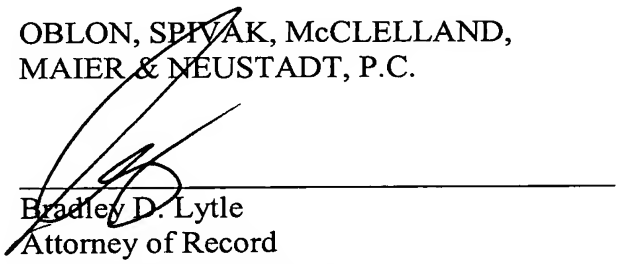
Therefore, Ofek fails to teach or suggest "***receiving a request from a receiver device*** to add identification information to said set packet data ***only during a predetermined period***" and "adding said requested identification information to said sent packet data during said predetermined period and ***not adding identification information during periods other than said predetermined period,***" as recited in amended independent Claim 1.

Accordingly, Applicant respectfully requests that the rejection of Claim 1 (and Claims 2 and 3 which depend therefrom) under 35 U.S.C. § 103(e) be withdrawn. For substantially similar reasons, it is also submitted that amended independent Claim 4 patentably defines over Ofek.

Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1-4 is patentably distinguishing over the applied references. The present application is therefore believed to be in condition for allowance and an early and favorable reconsideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Andrew T. Harry
Registration No. 56,959

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\ATH\PROSECUTION\24'S\247926US\247926US-AMDDUE62107.DOC